IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Thomas FRIETSCH	**Confirmation No.:**	7146
Serial No.:	10/698,016	**Examiner:** Thomas J. DAILEY	
Filed:	October 31, 2003	**Group Art Unit:**	2452

Title: NETWORK SERVER AND METHOD OF DISCOVERY OF A NETWORK
          NODE

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office

Action mailed November 16, 2011, and in connection with the Notice of Appeal filed on

February 16, 2012.

It is respectfully submitted that the present application has been at least twice rejected.

Each of the topics required in an Appeal Brief and a Table of Contents are presented

herewith and labeled appropriately.

TABLE OF CONTENTS

(1)   Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

(2)   Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3)   Summary of Claimed Subject Matter

Claims 32, 35, 40, 43, and 46 are the independent claims in this appeal. It should be understood that the citations below to the original disclosure as providing support for the claimed features are merely exemplary and do not limit the claim features to only those citations.

Claim 32.   A method of discovering that a particular network node (Network Node 102 in Fig. 1) has been connected to a computer network, wherein the network includes (a) plural nodes, one of which is the particular node, and (b) a server arrangement including a network portion (Network Server 100 in Fig. 1) and a discovery portion (Discovery Server 112 in Fig. 1), the method comprising:

responding to an establishment of a connection of the particular network node to the network, the network portion of the server arrangement receiving an access request from the particular network node, wherein the particular network node has an assigned address assigned by a device in the network (106 in Fig. 1; *Specification*, paragraphs [0015] and [0019]);

in response to receiving the access request, the network portion authenticating the particular network node (*Specification*, paragraphs [0015] and [0019]);

the network portion (100) sending a discovery request and the assigned address of the particular network node to the discovery portion (112) of the server arrangement after the network portion has successfully authenticated the particular network node (110 in Fig. 1; *Specification*, paragraphs [0016] and [0021]);

the discovery portion (112) storing the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for that particular network node (*Specification*, paragraphs [0016] and [0021]);

the discovery procedure for the particular network node, initiated by the discovery request from the network portion (100), including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node (*Specification*, paragraph [0018]).

Claim 35.   A method of discovering that a particular network node (Network Node 102 in Fig. 1) has been connected to a computer network, wherein the network includes (a) plural

nodes, one of which is the particular node, and (b) a server arrangement including a network

portion (Network Server 100 in Fig. 1) and a discovery portion (Discovery Server 112 in Fig. 1),

the method comprising:

responding to an establishment of a connection of the particular network node to the

network, the network portion of the server arrangement receiving an access request from the

particular network node, wherein the particular network node has an assigned address assigned

by a device in the network (106 in Fig. 1; *Specification*, paragraphs [0015] and [0019]);

in response to receiving the access request, the network portion authenticating the

particular network node (*Specification*, paragraphs [0015] and [0019]);

the network portion sending a discovery request and the assigned address of the particular

network node to the discovery portion of the server arrangement after the network portion has

successfully authenticated the particular network node (110 in Fig. 1; *Specification*, paragraphs

[0016] and [0021]);

the discovery portion storing the assigned address of the particular network node and

initiating a discovery program that performs a discovery procedure for the particular network

node (*Specification*, paragraphs [0016] and [0021]);

the discovery procedure for the particular network node, initiated by the discovery

request from the network portion, including polling other nodes in the network to determine a

network topology, the polled network topology including at least some of the other nodes to

which the particular network node is connected, and to determine the configuration of the

particular network node (*Specification*, paragraph [0018]).

Claim 40.   A server arrangement including machine-readable information executed by a

processor, the server arrangement for discovering that a particular network node (Network Node

102 in Fig. 1) has been connected to a computer network, wherein the particular network node

has an assigned address assigned by a device in the network, the server arrangement including:

a network portion (Network Server 100 in Fig. 1) and a discovery portion (Discovery

Server 112 in Fig. 1);

the network portion being arranged to, responding to an establishment of a connection of

the particular network node to the network, receive an access request from the particular network

node (106 in Fig. 1; *Specification*, paragraphs [0015] and [0019]);

the network portion being arranged to authenticate the particular network node in

response to receiving the access request (*Specification*, paragraphs [0015] and [0019]);

the network portion being arranged to send a discovery request and the assigned address

of the particular network node to the discovery portion after the network portion has successfully

authenticated the particular network node (110 in Fig. 1; *Specification*, paragraphs [0016] and

[0021]);

the discovery portion being arranged to store the assigned address of the particular

network node and initiating a discovery program that performs a discovery procedure for the

particular network node (*Specification*, paragraphs [0016] and [0021]); and

the discovery procedure for the particular network node, initiated by the discovery

request from the network portion, including polling other nodes in the network to determine a

network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node (*Specification*, paragraph [0018]).

Claim 43.   A server arrangement including machine-readable information executed by a processor, the server arrangement for discovering that a particular network node (Network Node 102 in Fig. 1) has been connected to a computer network, wherein the particular network node has an address assigned by a device in the network, the server arrangement including:

a network portion (Network Server 100 in Fig. 1) and a discovery portion (Discovery Server 112 in Fig. 1);

the network portion being arranged to, responding to an establishment of a connection of the particular network node to the network, receive an access request from the particular network node (106 in Fig. 1; *Specification*, paragraphs [0015] and [0019]);

the network portion being arranged to authenticate the particular network node in response to receiving the access request (*Specification*, paragraphs [0015] and [0019]);

the network portion being arranged to send a discovery request and the assigned address of the particular network node to the discovery portion after the network portion has successfully authenticated the particular network node (110 in Fig. 1; *Specification*, paragraphs [0016] and [0021]);

the discovery portion being arranged to store the assigned address of the particular

network node and initiating a discovery program that performs a discovery procedure for the

particular network node (*Specification*, paragraphs [0016] and [0021]);

the discovery procedure for the particular network node, initiated by the discovery

request from the network portion, including polling other nodes in the network to determine a

network topology, the polled network topology including at least some of the other nodes to

which the particular network node is connected, and to determine the configuration of the

particular network node (*Specification*, paragraph [0018]).

Claim 46.   A computer network for discovering that a particular network node has been

connected to the computer network, the network comprising:

a server arrangement including machine-readable information executed by a processor;

and

plural nodes, one of which is the particular network node (Network Node 102 in Fig. 1),

wherein the particular network node is assigned an addressed by the network;

the server arrangement including:

a network portion (Network Server 100 in Fig. 1) and a discovery portion

(Discovery Server 112 in Fig. 1), the network portion being arranged to, responding to an

establishment of a connection of the particular network node to the network, receive an access

request from the particular network node,

the network portion being arranged to authenticate the particular network node in response to receiving the access request (*Specification*, paragraphs [0015] and [0019]),

the network portion being arranged to send a discovery request and the assigned address of the particular network node to the discovery portion after the network portion has successfully authenticated the particular network node (110 in Fig. 1; *Specification*, paragraphs [0016] and [0021]),

the discovery portion being arranged to store the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for the particular network node (*Specification*, paragraphs [0016] and [0021]), and

the discovery procedure for the particular network node, initiated by the discovery request from the network portion, including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node (*Specification*, paragraph [0018]).

(4)   **Arguments**

   A.   **The rejection of claims 32, 33, 35, 36, 38–41, 43, 44, 46, and 47 under 35**

U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No.

2002/0010767 to Farrow et al. (hereinafter Farrow) in view of U.S. Patent Application

Publication No. 2003/0005100 to Barnard et al. (hereinafter Barnard), and further in view

of U.S. Patent No. 5,710,885 to Bondi (hereinafter "Bondi") should be reversed.

   The test for determining if a claim is rendered obvious by one or more references for

purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex*

Inc., 550 U.S. 398, 82 USPQ2d 1385 (2007):

   "Under §103, the scope and content of the prior art are to be determined;
   differences between the prior art and the claims at issue are to be ascertained; and
   the level of ordinary skill in the pertinent art resolved. Against this background
   the obviousness or nonobviousness of the subject matter is determined. Such
   secondary considerations as commercial success, long felt but unsolved needs,
   failure of others, etc., might be utilized to give light to the circumstances
   surrounding the origin of the subject matter sought to be patented." Quoting
   Graham v. John Deere Co. of Kansas City, 383 U.S. 1 (1966).

   According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C.

103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526,

57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a

determination of whether the claims would have been obvious to one of ordinary skill in the art

based on any one of the following proper rationales:

   (A) Combining prior art elements according to known methods to yield
   predictable results; (B) Simple substitution of one known element for another to
   obtain predictable results; (C) Use of known technique to improve similar devices
   (methods, or products) in the same way; (D) Applying a known technique to a
   known device (method, or product) ready for improvement to yield predictable

results; (E) "Obvious to try"—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Furthermore, as set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385.

Claims 32, 33, 35, 36, 38-41, 43, 44, 46, and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Farrow in view of Barnard, and further in view of Bondi. The rejection should be reversed for at least the following reasons.

- Independent Claim 32:

  Independent claim 32 recites, *inter alia*,

  responding to an establishment of a connection of the particular network node to the network, <u>the network portion of the server arrangement receiving an access request from the particular network node</u>, wherein the particular network node has an assigned address assigned by a device in the network. (*Emphasis added*)

In setting forth the rejection of claim 32, the Examiner asserts that the features recited

above are disclosed by Farrow, paragraph [0036], lines 6-13 (*Final Office Action*, page 4).

However, that assertion is respectfully traversed because, in paragraph [0036], lines 6-13,

Farrow states,

> First a client 208 requests an IP address from the DHCP server 203N on
> the network, step 801. The DHCP server 203N dynamically assigns the client 208
> an IP address before it has been authenticated, step 802. The client 208 then issues
> a registration request with the binding server 209 and communicates its userid,
> password and the IP address it just obtained from the DHCP server 203N to the
> binding server 209, step 803. (*Emphasis added*)

As such, in paragraph [0036], Farrow discloses that the client 208 sends a registration

request to the binding server 209 to register the IP address. Thus, the "registration request" in

Farrow is a request to register the IP address, and not to access the network. Accordingly, the

binding server 209 of Farrow receives a registration request, and does not receive an "access

request" from a client. Therefore, contrary to the assertion by the Examiner, Farrow fails to

teach or suggest "the network portion of the server arrangement receiving an access request from

the particular network node," as recited in independent claim 32.

Independent claim 32 also recites,

> the network portion sending a discovery request and the assigned address
> of the particular network node to the discovery portion of the server arrangement
> after the network portion has successfully authenticated the particular network
> node. (*Emphasis added*)

In the rejection of claim 32, the Examiner asserts that the features recited above are

disclosed by Farrow, paragraph [0036], lines 35-43 (*Final Office Action*, page 4). More

specifically, in paragraph [0036], lines 35-43, Farrow discloses that the binding server 209 sends

authenticated credentials to be stored in the central database 204. The Examiner asserts that the

sending of the authenticated credentials from the binding server 209 to the central database 204

is equivalent to "the network portion <u>sending a discovery request</u> and the assigned address of the

particular network node <u>to the discovery portion of the server arrangement</u> after the network

portion has successfully authenticated the particular network node," as recited in independent

claim 32. *Id.* The Examiner also asserts that the central database 204 of Farrow is equivalent to

the "discovery portion" recited in independent claim 32. *Id.*

However, those assertions are respectfully traversed because, in Farrow, the

"authenticated credentials" that the binding server 209 sends to the central database 204 are not a

discovery request. Instead, the authenticated credentials include the IP address, user id, and

password (See *Farrow*, paragraph [0036], lines 10-13). None of the IP address, user id, and

password is a request for discovery. Thus, the authenticated credentials in Farrow are not

equivalent to the "discovery request" recited in claim 32.

In addition, in Farrow, the central database 204 is for storing data, such as the

authenticated credentials of client devices. The central database 204 of Farrow does not and

cannot perform or initiate a discovery procedure to determine a topology of a node. Thus, the

central database 204 in Farrow is not equivalent to the "discovery portion" recited in claim 32.

As such, in Farrow, the binding server 209 may send authenticated credentials to be

stored in the central database 204; however, the binding server 209 does not send a discovery

request to a discovery portion, as recited in claim 32. Therefore, Farrow fails to teach or suggest,

"<u>the network portion sending a discovery request and the assigned address of the particular</u>

network node to the discovery portion of the server arrangement after the network portion has

successfully authenticated the particular network node," as recited in independent claim 32.

Independent claim 32 also recites,

the discovery portion storing the assigned address of the particular
network node and initiating a discovery program that performs a discovery
procedure for that particular network node;
the discovery procedure for the particular network node, initiated by the
discovery request from the network portion, including polling other nodes in the
network to determine a network topology, the polled network topology including
at least some of the other nodes to which the particular network node is
connected, and to determine the configuration of the particular network node.
(*Emphasis added*)

In setting forth the rejection of claim 32, the Examiner correctly admits that Farrow fails

to teach or suggest the features recited above (*Final Office Action*, page 5).

The Examiner then asserts that Barnard discloses in paragraph [0077], lines 11-22, "the

discovery portion ... initiating a discovery program that performs a discovery procedure for that

particular network node" in response to the supplying of the discovery request and the assigned

address of the particular node to the discovery portion, as recited above in claim 32 (*Final Office

Action*, bottom of page 5).

However, that assertion is respectfully traversed because, in paragraph [0077], lines 11-

22, Barnard discloses that the discovery module 84 sends an SNMP information request to a

printing device 18, and the printing device 18 sends the discovery module the requested SNMP

information, such as the printing device's MAC address, IP address, and printing device type.

As such, in Barnard, the discovery module 84 sends a client device a request for

information such as the IP address and MAC address. However, such disclosure of Barnard

14

would not have worked in Farrow. Specifically, as discussed above, the Examiner asserts that

the "central database 204" of Farrow that stores the IP address and MAC address of the client

device 208 is a "discovery portion" (See *Final Office Action*, page 4). Thus, the central database

204 of Farrow already contains the IP address of the client device. As a result, the central

database 204 of Farrow would not send a request to the client device for the client device's IP

address. Therefore, one of ordinary skill in the art would not have utilized the functions of the

discovery module 84, as disclosed by Barnard, for the central database 204 of Farrow.

Accordingly, even if assuming for the sake of argument that one skilled in the art were somehow

motivated to combine Farrow and Barnard, that person in the art would not utilize the discovery

module 84, or its functions, disclosed by Barnard into the central database 204 of Farrow.

Therefore, the proposed combination of Farrow in view of Barnard fails to teach or suggest "the

discovery portion storing the assigned address of the particular network node and initiating a

discovery program that performs a discovery procedure for that particular network node," as

recited in independent claim 32.

For at least the foregoing reasons, independent claim 32 is *not* obvious in view of the

proposed combination of Farrow in view of Barnard and Bondi. Therefore, reversal of the

rejection of independent claim 32 and allowance of the claim is respectfully requested.

- Independent Claims 35, 40, 43, and 46:

    Independent claims 35, 40, 43, and 46 recite features similar to those of independent

claim 32 as discussed above. Thus, independent claims 35, 40, 43, and 46 are also believed to

be allowable over the cited documents of record for at least the same reasons as set forth above
in connection with independent claim 32. It is therefore respectfully requested that the rejection
of independent claims 35, 40, 43, and 46 be reversed, and these claims be allowed.

- Dependent Claims 33, 36, 38, 39, 41, 44, and 47:

     Claims 33, 36, 38, 39, 41, 44, and 47 are dependent from one of independent claims 32,
35, 40, 43, and 46. Thus, they are also believed to be allowable over the cited documents of
record for at least the same reasons as set forth above in connection with independent claims 32,
35, 40, 43, and 46. It is therefore respectfully requested that the rejection of claims 33, 36, 38,
39, 41, 44, and 47 be reversed, and these dependent claims be allowed.

**B.   The rejection of claims 34, 37, 42, and 45 under 35 U.S.C. §103(a) as being
unpatentable over Farrow in view of Barnard and Bondi, and further in view of what was
well known in the art at the time of the invention should be reversed.**

     Claims 34, 37, 42 and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable
over Farrow in view of Barnard and Bondi, and further in view of what was well known in the
art at the time of the invention.

     Claims 34, 37, 42 and 45 are dependent from one of independent claims 32, 35, 40, and
43. Thus, they are believed to be allowable for at least the same reasons as set forth above in
connection with independent claims 32, 35, 40, and 43. It is therefore requested that the
rejection of claims 34, 37, 42 and 45 be reversed, and these claims be allowed.

(5)   Conclusion

For at least the reasons given above, the rejection of claims 32-47 described above should

be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with

this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: April 16, 2012   By   /Ashok K. Mannava/
                                       Ashok K. Mannava
                                       Registration No. 45,301
                                       (703) 652-3822

                                       MANNAVA & KANG, P.C.
                                       11240 Waples Mill Road
                                       Suite 300
                                       Fairfax, VA 22030
                                       (703) 865-5150 (facsimile)

(6)   Claims Appendix

32.   (Previously Presented) A method of discovering that a particular network node has been connected to a computer network, wherein the network includes (a) plural nodes, one of which is the particular node, and (b) a server arrangement including a network portion and a discovery portion, the method comprising:

responding to an establishment of a connection of the particular network node to the network, the network portion of the server arrangement receiving an access request from the particular network node, wherein the particular network node has an assigned address assigned by a device in the network;

in response to receiving the access request, the network portion authenticating the particular network node;

the network portion sending a discovery request and the assigned address of the particular network node to the discovery portion of the server arrangement after the network portion has successfully authenticated the particular network node;

the discovery portion storing the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for that particular network node;

the discovery procedure for the particular network node, initiated by the discovery request from the network portion, including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to

which the particular network node is connected, and to determine the configuration of the
particular network node.

33.   (Previously Presented) The method of claim 32 wherein the discovery portion receives a
sequence of discovery requests including assigned addresses of various nodes of the network
which have requested access to the network, the discovery portion storing the assigned addresses
of the received requests from the various nodes.

34.   (Previously Presented) The method of claim 33 wherein the discovery portion stores the
assigned addresses as a stack that the discovery portion processes in a first-in-first-out order.

35.   (Previously Presented) A method of discovering that a particular network node has been
connected to a computer network, wherein the network includes (a) plural nodes, one of which is
the particular node, and (b) a server arrangement including a network portion and a discovery
portion, the method comprising:

        responding to an establishment of a connection of the particular network node to the
network, the network portion of the server arrangement receiving an access request from the
particular network node, wherein the particular network node has an assigned address assigned
by a device in the network;

        in response to receiving the access request, the network portion authenticating the
particular network node;

the network portion sending a discovery request and the assigned address of the particular network node to the discovery portion of the server arrangement after the network portion has successfully authenticated the particular network node;

the discovery portion storing the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for the particular network node;

the discovery procedure for the particular network node, initiated by the discovery request from the network portion, including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node.

36.   (Previously Presented) The method of claim 35 wherein the discovery portion receives a sequence of discovery requests including assigned addresses of various nodes of the network which have requested access to the network, the discovery portion storing the assigned addresses of the received requests from the various nodes.

37.   (Previously Presented) The method of claim 36 wherein the discovery portion stores the assigned addresses as a stack that the discovery portion processes in a first-in-first-out order.

38.   (Previously Presented) A non-transitory storage medium or device storing machine-readable information for causing a processor to execute the steps of claim 32 on the network of claim 32.

39.   (Previously Presented) A non-transitory storage medium or device storing machine-readable information for causing a processor to execute the steps of claim 35 on the server arrangement of claim 35.

40.   (Previously Presented) A server arrangement including machine-readable information executed by a processor, the server arrangement for discovering that a particular network node has been connected to a computer network, wherein the particular network node has an assigned address assigned by a device in the network, the server arrangement including:

a network portion and a discovery portion;

the network portion being arranged to, responding to an establishment of a connection of the particular network node to the network, receive an access request from the particular network node;

the network portion being arranged to authenticate the particular network node in response to receiving the access request;

the network portion being arranged to send a discovery request and the assigned address of the particular network node to the discovery portion after the network portion has successfully authenticated the particular network node;

the discovery portion being arranged to store the assigned address of the particular

network node and initiating a discovery program that performs a discovery procedure for the

particular network node; and

the discovery procedure for the particular network node, initiated by the discovery

request from the network portion, including polling other nodes in the network to determine a

network topology, the polled network topology including at least some of the other nodes to

which the particular network node is connected, and to determine the configuration of the

particular network node.

41.   (Previously Presented) The server arrangement of claim 40 wherein the discovery

portion is arranged to receive a sequence of discovery requests including assigned addresses of

various nodes of the network which have requested access to the network and includes a storage

for storing the assigned addresses on the received requests from the various nodes.

42.   (Previously Presented) The server arrangement of claim 41 wherein the storage is

arranged to store the assigned addresses as a stack, the discovery portion being arranged to

process the stack in a first-in-first-out order.

43.   (Previously Presented) A server arrangement including machine-readable information

executed by a processor, the server arrangement for discovering that a particular network node

has been connected to a computer network, wherein the particular network node has an address assigned by a device in the network, the server arrangement including:

a network portion and a discovery portion;

the network portion being arranged to, responding to an establishment of a connection of the particular network node to the network, receive an access request from the particular network node;

the network portion being arranged to authenticate the particular network node in response to receiving the access request;

the network portion being arranged to send a discovery request and the assigned address of the particular network node to the discovery portion after the network portion has successfully authenticated the particular network node;

the discovery portion being arranged to store the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for the particular network node;

the discovery procedure for the particular network node, initiated by the discovery request from the network portion, including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node.

44.   (Previously Presented) The server arrangement of claim 43 wherein the discovery

portion is arranged to receive a sequence of discovery requests including assigned addresses of

various nodes of the network which have requested access to the network and includes a storage

for storing the assigned addresses on the received requests from the various nodes.

45.   (Previously Presented) The server arrangement of claim 44 wherein the storage is

arranged to store the assigned addresses as a stack, the discovery portion being arranged to

process the stack in a first-in-first-out order.

46.   (Previously Presented) A computer network for discovering that a particular network

node has been connected to the computer network, the network comprising:

        a server arrangement including machine-readable information executed by a processor;

and

        plural nodes, one of which is the particular network node, wherein the particular network

node is assigned an addressed by the network;

        the server arrangement including:

                a network portion and a discovery portion, the network portion being arranged to,

responding to an establishment of a connection of the particular network node to the network,

receive an access request from the particular network node,

                the network portion being arranged to authenticate the particular network node in

response to receiving the access request,

the network portion being arranged to send a discovery request and the assigned address of the particular network node to the discovery portion after the network portion has successfully authenticated the particular network node,

the discovery portion being arranged to store the assigned address of the particular network node and initiating a discovery program that performs a discovery procedure for the particular network node, and

the discovery procedure for the particular network node, initiated by the discovery request from the network portion, including polling other nodes in the network to determine a network topology, the polled network topology including at least some of the other nodes to which the particular network node is connected, and to determine the configuration of the particular network node.

47.   (Previously Presented) The computer network of claim 46 wherein the discovery portion is arranged to receive a sequence of discovery requests including assigned addresses of various nodes of the network which have requested access to the network and includes a storage for storing the assigned addresses on the received requests from the various nodes.